# Resilient and Privacy-Preserving Leader-Follower Consensus in Presence of Cyber-Attacks

Azwirman Gusrialdi, *Member, IEEE*

***Abstract*—This letter presents a novel and unified distributed control framework that ensures resilient leader-follower consensus in the presence of unknown but bounded attacks on both the communication network and actuators while simultaneously preserving the privacy of an agent's physical state from eavesdroppers. To this end, a virtual state and time-varying signals are introduced to each agent, which function as masks to the physical state and are designed to ensure resilient leader-follower consensus. The proposed control strategy does not require high network connectivity and imposes no restrictions on the number of attacks. A numerical example is provided to illustrate the results.**

***Index Terms*—Leader-follower consensus, resilient distributed protocols, privacy, cyber-attacks.**

## I. Introduction

LEADER-FOLLOWER consensus is a class of cooperative control systems that find applications in various fields, such as intelligent transportation systems, smart grid, and robotic network [1], [2], [3], [4] due to its scalability and robustness to a single point of failure. However, the reliance on a communication network exposes the cooperative system to cyber-attacks [5]. An attacker could inject malicious signals into the communication links, degrading system performance and in the worst case causing system-wide instability [6]. In addition, information exchanged through wireless or wired communication channels is vulnerable to eavesdroppers, which include external adversary and honest-but-curious node aiming to steal sensitive information from an individual system. Thus, it is crucial to ensure both the resilient operation of the leader-follower consensus in the presence of unknown cyber-attacks and the protection of private data from eavesdroppers.

Leader-follower consensus in presence of cyber-attacks has received significant attention in the last decade. One potential approach to address this issue is by identifying compromised nodes or communication links and subsequently removing them [7], [8]. However, the strategy requires high network connectivity, which depends on the number of compromised links, to ensure consensus. An alternative strategy, the mean subsequence reduced algorithm, has been proposed for leader-follower consensus in the presence of misbehaving agents [9], [10]. This method does not assume any specific behaviour from the attacker and does not require the healthy agent to detect the misbehaving agents. However, it often comes with restrictions on the number of compromised nodes and the connectivity of the communication network. Furthermore, this method is not effective in ensuring consensus when only the communication network is compromised. In the literature, various alternative strategies have been proposed to address the limitations of high network connectivity and restrictions on the number of attacks, see, e.g., [11], [12], [13], [14], [15], [16]. For instance, the work [14], [16] propose resilient leader-following consensus under Denial-of-Service (DoS) attacks on the communication links. While the individual agent in those work has linear or non-linear dynamics, the type of attacks is only limited to DoS attacks which are less sophisticated than the false data injection (FDI) attacks. On the other hand, the work [12], [13], [15] present approaches for resilient leader-follower consensus under FDI attacks on the communication links. However, the work do not consider attacks on the node's actuator.

It is worth to note that all the strategies proposed in the above-mentioned works rely on exchanging the physical states of both the followers and the leader. This exchange of information can lead to the disclosure of an agent's physical state, making the cooperative system vulnerable to potential privacy threats posed by eavesdroppers. To tackle this privacy concern, the authors in [17] propose a privacy-preserving leader-follower consensus algorithm. However the strategy does not guarantee the resiliency of the cooperative system. Cryptography-based methods, see, e.g., [18], [19] have been proposed for leader-follower consensus to ensure the privacy of an agent's physical state. However, these strategies have notable limitations. They might suffer from high computational complexity and some require the existence of trusted or legitimate agents, which might not always be feasible. More importantly, these methods do not ensure the resiliency of cooperative systems against unknown injections. The authors in [19], [20] propose strategies that ensure both resiliency and privacy requirements. However, these strategies are limited to leaderless consensus and impose restrictions on the attack's model including the number of

Manuscript received 14 June 2023; revised 29 July 2023; accepted 20 August 2023. Date of publication 24 August 2023; date of current version 8 September 2023. This work was supported by the Academy of Finland under Project 330073. Recommended by Senior Editor K. Savla.

The author is with the Automation and Mechanical Engineering Unit, Tampere University, 33720 Tampere, Finland (e-mail: azwirman.gusrialdi@tuni.fi).

Digital Object Identifier 10.1109/LCSYS.2023.3308144

attacks. Furthermore, the methods also require high network connectivity.

From the preceding discussions, it is evident that attack-resilient and privacy-preserving leader-follower consensus have mostly been treated as two separate issues. This letter introduces a novel *unified* control framework that addresses both problems simultaneously. The framework ensures resilient leader-follower consensus in the presence of FDI attacks on both the actuators and communication links while also protecting an agent's physical state from eavesdroppers. To this end, each agent maintains a virtual state and utilizes local time-varying but uniformly bounded signals. These virtual state and time-varying signals act as mask for the physical state, effectively preserving the physical state's privacy of both the leader and followers from eavesdroppers. Moreover, the virtual state and time-varying signals are designed to ensure the approximate leader-follower consensus in the presence of unknown but bounded attacks. The proposed resilient control does not require high network connectivity and does not impose any restrictions on the number of attacks.

This letter is organized as follows. After formally formulating the problem in Section II, the proposed resilient and privacy-preserving leader-follower consensus is presented and analyzed in Section III. The proposed algorithm is demonstrated via a numerical example in Section IV. Concluding remarks are presented in Section V.

*Notation:* Let $\mathbb{R}$ be the set of real numbers; vector $\mathbf{1}_n \in \mathbb{R}^n$ denotes the vector of all ones and $I_n \in \mathbb{R}^{n\times n}$ denotes an $n \times n$ identity matrix. Cardinality of a set $\mathcal{N}$ is denoted by $|\mathcal{N}|$. The $i$th eigenvalue of a square matrix $A$ can be written as $\lambda_i(A) = a_i + b_i\iota$ where $a_i = \Re(\lambda_i(A))$ is the real-part of $\lambda_i(A)$, $b_i = \Im(\lambda_i(A))$ is the imaginary-part of $\lambda_i(A)$, and $\iota = \sqrt{-1}$. Superscript "$T$" represents the transpose of a matrix or a vector.

## II. Problem Formulation

Consider a cooperative system consisting of $n+1$ nodes where a leader node is labeled by 0 and the follower nodes are labeled by $i = 1, \ldots, n$. The communication network topology among the leader and follower nodes is modelled as a directed graph $\mathcal{G} = \{\mathcal{V}, \mathcal{E}\}$ where $\mathcal{V} = \{v_0, v_1, \ldots, v_n\}$ and $\mathcal{E} \subset \mathcal{V} \times \mathcal{V}$ represent the node set and edge/link set respectively. A directed edge $(j, i) \in \mathcal{E}$ means that node $i$ can receive information from node $j$. The neighbours of node $i$ is defined as $\mathcal{N}_i = \{j | (j, i) \in \mathcal{E}\}$. A directed path from node $i$ to node $j$ is a sequence of consecutive edges $\{(v_i, v_m), (v_m, v_q), \ldots, (v_l, v_j)\}$.

Let $x_i(t) \in \mathbb{R}$ denote the physical state of node $i$ whose dynamics is given by

$$\begin{aligned} \dot{x}_0(t) &= f(x_0(t)), \\ \dot{x}_i(t) &= u_i\Big(\ell_i(t), \{y_j^i(t)\}\Big), \quad i = 1, \ldots, n, \quad j \in \mathcal{N}_i, \end{aligned} \tag{1}$$

where $u_i$ is the control input, $\ell_i(t)$ denotes the local information of node $i$ and $y_j^i(t)$ denotes the information that node $j$ sends to node $i$ via the communication network. The dynamics of the leader node $v_0$ satisfies the following assumption.

*Assumption 1:* The derivative of $x_0$ is uniformly bounded, that is $|f(x_0(t))| \leq \zeta$ where $\zeta$ is a positive constant.

*Remark 1:* The results in this letter can be extended in a straightforward manner to the case $x_i(t) \in \mathbb{R}^p$ by using the Kronecker product. When the individual dynamics of the follower nodes are given by a heterogeneous nonlinear/linear system, one can potentially use the idea presented in [21], [22]. Specifically, if the individual dynamics can become input passivity-short by a local feedback controller, the dynamic behaviours of the follower nodes at the network level as well as their network control design can then be transformed to (1).

We make the following assumption on the communication network topology.

*Assumption 2:* The leader node $v_0$ has a directed path to every follower node.

In practice, the actuators of the follower nodes and the communication channels are vulnerable to cyber-attacks. In this letter, we consider false data injection (FDI) attacks on both the actuators and communication channels. Specifically, the attack on a follower node's actuator is modelled as

$$\tilde{u}_i(t) = u_i(t) + \delta_{ui}(t), \tag{2}$$

where $\tilde{u}_i(t)$ is the compromised control input under unknown injection $\delta_{ui}(t)$. Furthermore, follower node $i$ may not receive the true information from its neighboring node $j$, that is the possibly corrupted information that node $i$ is receiving from its neighbouring node $j$, including the leader node, takes the following form

$$\tilde{y}_j^i(t) = y_j^i(t) + \delta_{ji}(t), \ j \in \mathcal{N}_i, \tag{3}$$

where $\delta_{ji}(t)$ is the malicious injection into the communication link $(j, i) \in \mathcal{E}$. The unknown injections $\delta_{ui}(t)$, $\delta_{ji}(t)$ satisfy the following assumption.

*Assumption 3:* The injections $\delta_{ui}(t)$, $\delta_{ji}(t)$ are both uniformly bounded.

*Remark 2:* Assumption 3 is reasonable in practical scenarios and has been considered in several studies, e.g., [23], [24]. Moreover, no restrictions are made on the number of attacks and in contrast to the setup in [10], [11], [25], we assume that the communication links from the leader to the follower nodes can also be compromised.

In addition to considering FDI attacks, our work also takes into account the presence of eavesdroppers, which are external adversaries with the objective of stealing information on the physical states $x_i(t)$ of all nodes including the leader by tapping the communication links. Furthermore, we also consider the existence of an honest-but-curious node, which seeks to estimate the physical state $x_i(t)$ of its neighbouring nodes. To illustrate this scenario, we adopt an example from [17], which involves the transportation of critical materials by a group of trucks to a destination designated by an operator (leader node), as depicted in Fig. 1. Both the leader node and the trucks share the same goal of protecting their state $x_i(t)$ from being disclosed to the eavesdroppers.

The objective of this letter is to design the control input $u_i(t)$ such that the cooperative system in (1) reaches an approximate consensus, that is

$$\Big|\lim_{t\to\infty} x_i(t) - x_0(t)\Big| \leq \epsilon, \ i = 1, \ldots, n, \tag{4}$$

where $\epsilon$ is a small positive scalar. Furthermore, the nodes including the leader node must also preserve the privacy of

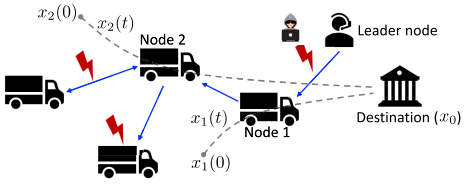


Fig. 1. The transportation of critical materials by a group of trucks to a destination designated by an operator (leader node). The solid lines represent communication links and the dashed lines denote the routes of the trucks. The actuator and communication network are subject to unknown injections. Furthermore, the communication network is also vulnerable to eavesdroppers who aim to steal information on $x_i(t)$.

their physical states, that is to prevent the eavesdroppers from learning accurately $x_j(t)$ from the information $y^i_j(t)$.

*Remark 3:* The acceptable value of $\epsilon$ in (4) in practice depends on the application of interest. For example, in the problem of frequency synchronization in the power grid and islanded microgrid applications, according to National Grid ESO in the U.K., the steady-state frequency must be within the limits of 49.5 Hz to 50.5 Hz. This means that $\epsilon = 0.5$ Hz.

## III. Main Results

In order to ensure resilient leader-follower consensus and preserve privacy of the physical states, we introduce a virtual state $z_j(t) \in \mathbb{R}$ and time-varying but uniformly bounded signals $p^i_{j,1}(t), p^i_{j,2}(t) \in \mathbb{R}$ to the $j$-th node with $j = 0, 1, \ldots, n$. The virtual state of the leader node $v_0$ has dynamics $\dot{z}_0(t) = g(z_0(t))$ where $\dot{z}_0(t)$ is uniformly bounded. The signals $p^i_{j,1}(t), p^i_{j,2}(t) \in \mathbb{R}$ are chosen independently by node $j$, and along with the virtual state $z_j(t)$, they are used to mask the physical state $x_j(t)$ before being transmitted to node $i$ where $j \in \mathcal{N}_i$. Specifically, node $j$ sends the following masked physical states $y^i_{j,1}(t), y^i_{j,2}(t)$ to node $i$:

$$\begin{aligned} y^i_{j,1}(t) &= x_j(t) - \beta z_j(t) + p^i_{j,1}(t), \\ y^i_{j,2}(t) &= \gamma z_j(t) + \beta x_j(t) + p^i_{j,2}(t), \ j = 0, 1, \ldots, n \end{aligned} \tag{5}$$

where $\beta > 0, \gamma > 0$ are scalar gains designed to ensure resiliency against malicious injections. In contrast to the physical state $x_i(t)$, the virtual states $z_i(t)$ do not have any physical meanings and $z_i(0)$ can be set to any values. Next, using the virtual state $z_i(t)$, the local information of each follower node $\ell_i(t)$ in (1) is defined by

$$\begin{aligned} \ell_{i,1}(t) &= -|\mathcal{N}_i|(x_i(t) - \beta z_i(t)), \\ \ell_{i,2}(t) &= -|\mathcal{N}_i|(\beta x_i(t) + \gamma z_i(t)). \end{aligned} \tag{6}$$

Finally, the proposed control input for cooperative system (1) which achieves the objective (4) while preserving the privacy of physical states $x_i(t)$ is given by

$$u_i(t) = \ell_{i,1}(t) + \sum_{j=0}^{n} a_{ij} y^i_{j,1}(t), \ i = 1, \ldots, n \tag{7}$$

where $a_{ij} = 1$ if follower node $i$ can receive information from node $j$ and $a_{ij} = 0$ otherwise. Furthermore, the virtual state of the follower node $z_i(t)$ is updated according to

$$\dot{z}_i(t) = \ell_{i,2}(t) + \sum_{j=0}^{n} a_{ij} y^i_{j,2}(t), \ i = 1, \ldots, n \tag{8}$$

where the information $\ell_{i,1}(t), \ell_{i,2}(t), y^i_{j,1}(t), y^i_{j,2}(t)$ are defined in (6) and (5).

The gains $\beta, \gamma$ are designed offline before deploying the cooperative systems while the information $\ell_i(t)$ (resp. $y^i_j(t)$) are computed (resp. shared) online. Regarding the information available to the eavesdropper, it is assumed that the external adversary listens to information $y^i_j(t)$ being exchanged among the agents and possibly knows the network topology. However, the adversary does not know the structure of (5)–(8) since they are considered as local information for each agent. On the other hand, since an honest-but-curious node is part of the cooperative system, he/she has access to the information $y^i_j(t)$ and the structure of (5)–(8) including gains $\beta, \gamma$.

*Remark 4:* In contrast to the resilient leader-follower consensus algorithm proposed in [13], control input (7), (8) results in a sparse communication network topology.

### A. Resilient Leader-Follower Consensus

In this subsection, we analyze the resiliency of the cooperative system under the proposed control input (7). To this end, the closed-loop dynamics of follower nodes (1) under control input (7) and virtual state's dynamics (8) in presence of unknown injections can be written as

$$\begin{aligned} \dot{x}_i &= -|\mathcal{N}_i|(x_i(t) - \beta z_i(t)) \\ &\quad + \sum_{j=0}^{n} a_{ij}\Big[x_j(t) - \beta z_j(t) + p^i_{j,1}(t) + \delta_{ji}(t)\Big] + \delta_{ui}(t) \\ \dot{z}_i &= -|\mathcal{N}_i|(\beta x_i(t) + \gamma z_i(t)) \\ &\quad + \sum_{j=0}^{n} a_{ij}\Big[\gamma z_j(t) + \beta x_j(t) + p^i_{j,2}(t) + \bar{\delta}_{ji}(t)\Big]. \end{aligned} \tag{9}$$

Here, it is assumed that the adversary can insert different injections $\delta_{ji}(t), \bar{\delta}_{ji}(t)$ into the exchanged information $y^i_{j,1}(t)$ and $y^i_{j,2}(t)$ respectively.

Defining vectors $x(t) = [x_1(t), \ldots, x_n(t)]^T$ and $z(t) = [z_1(t), \ldots, z_n(t)]^T$ we can write in a compact form the closed-loop system (9) for all the follower nodes as

$$\begin{aligned} \dot{x}(t) &= Ax(t) + Bx_0(t) - \beta Az(t) - \beta Bz_0(t) + d(t) \\ \dot{z}(t) &= \gamma Az(t) + \beta Ax(t) + \beta Bx_0(t) + \gamma Bz_0(t) + \bar{d}(t). \end{aligned} \tag{10}$$

The vectors $d(t) = [d_1(t), \ldots, d_n(t)]^T$ and $\bar{d}(t) = [\bar{d}_1(t), \ldots, \bar{d}_n(t)]^T$ are given by

$$d_i(t) = \delta_i(t) + \sum_{j=0}^{n} a_{ij} p^i_{j,1}(t), \quad \bar{d}_i(t) = \bar{\delta}_i(t) + \sum_{j=0}^{n} a_{ij} p^i_{j,2}(t)$$

where

$$\delta_i(t) = \delta_{ui}(t) + \sum_{j=0}^{n} a_{ij}\delta_{ji}(t), \quad \bar{\delta}_i(t) = \sum_{j=0}^{n} a_{ij}\bar{\delta}_{ji}(t). \tag{11}$$

Furthermore, matrix $A \in \mathbb{R}^{n\times n}$ is defined as

$$A = \begin{bmatrix} -\sum_{j=0}^{n} a_{1j} & a_{12} & \cdots & a_{1n} \\ a_{21} & -\sum_{j=0}^{n} a_{2j} & \cdots & a_{2n} \\ \vdots & & \ddots & \\ a_{n1} & a_{n2} & \cdots & -\sum_{j=0}^{n} a_{nj} \end{bmatrix}$$

while vector $B \in \mathbb{R}^{n\times 1}$ is defined as $B = [a_{10}, \ldots, a_{n0}]^T$. Assumption 2 implies that matrix $A$ is Hurwitz [26]. Furthermore, we have the following relationship $A\mathbf{1}_n = -B$.

Next, let us define the following error vectors

$$\tilde{x}(t) = x(t) - \mathbf{1}_n x_0(t), \quad \tilde{z}(t) = z(t) - \mathbf{1}_n z_0(t). \tag{12}$$

By noting that $A\mathbf{1}_n = -B$, dynamics of the error $\tilde{x}(t)$ can be calculated as

$$\begin{aligned}\dot{\tilde{x}}(t) &= A\tilde{x}(t) + (A\mathbf{1}_n + B)x_0(t) - \beta A\tilde{z}(t) - \beta(A\mathbf{1}_n + B)z_0(t)\\ &\quad + d(t) - \mathbf{1}_n f(x_0(t))\\ &= A\tilde{x}(t) - \beta A\tilde{z}(t) + d(t) - \mathbf{1}_n f(x_0(t)).\end{aligned}$$

Similarly, dynamics of the error $\tilde{z}(t)$ can also be calculated as

$$\dot{\tilde{z}}(t) = \gamma A\tilde{z}(t) + \beta A\tilde{x}(t) + \bar{d}(t) - \mathbf{1}_n g(z_0(t)).$$

Error dynamics $\tilde{x}(t), \tilde{z}(t)$ can be written in a compact form as

$$\begin{bmatrix}\dot{\tilde{x}}(t)\\ \dot{\tilde{z}}(t)\end{bmatrix} = \Phi\begin{bmatrix}\tilde{x}(t)\\ \tilde{z}(t)\end{bmatrix} + \begin{bmatrix}d(t) - \mathbf{1}_n f(x_0(t))\\ \bar{d}(t) - \mathbf{1}_n g(z_0(t))\end{bmatrix} \tag{13}$$

where $\Phi = \Omega \otimes A$ and

$$\Omega = \begin{bmatrix}1 & -\beta\\ \beta & \gamma\end{bmatrix}.$$

Before proceeding we introduce the following lemma.

*Lemma 1:* Under assumption 2 matrix $\Phi$ in (13) is Hurwitz for scalar gains $\beta > 0$ and $\gamma > 0$ satisfying

$$\gamma - 1 < 2\beta < \sqrt{\frac{(\gamma+1)^2 + \theta^2(\gamma-1)^2}{\theta^2}} \tag{14}$$

where $\theta = \max_i \frac{|\Im(\lambda_i(A))|}{|\Re(\lambda_i(A))|}$.

*Proof:* First, observe that for scalar gains $\beta, \gamma > 0$ satisfying the first inequality $2\beta > \gamma - 1$ in (14), the eigenvalues of matrix $\Omega$ are complex, i.e., $\lambda(\Omega) = r \pm \upsilon\iota$ where

$$r = \frac{1}{2}(\gamma+1), \quad \upsilon = \frac{1}{2}\sqrt{(2\beta)^2 - (\gamma-1)^2}.$$

Next, the eigenvalues of matrix $\Phi$ are in the set $S = \{\lambda(\Omega)\lambda_i(A) | i = 1, \ldots, n\}$. It follows that the real-part of the eigenvalues of $\Phi$ are given by

$$\begin{aligned}\Re(\lambda_i(\Phi)) &= \Re(\lambda(\Omega)\lambda_i(A))\\ &= r\Re(\lambda_i(A)) \pm \upsilon\Im(\lambda_i(A)).\end{aligned}$$

Recall that matrix $A$ is Hurwitz and thus $r\Re(\lambda_i(A)) < 0$. Hence, matrix $\Phi$ is Hurwitz, i.e., $\Re(\lambda_i(\Phi)) < 0$ for $i = 1, \ldots, n$ if and only if the following condition is satisfied

$$|r\Re(\lambda_i(A))| > |\upsilon\Im(\lambda_i(A))|$$

which can also be written as $\frac{r}{\upsilon} > \frac{|\Im(\lambda_i(A))|}{|\Re(\lambda_i(A))|}$, for $i = 1, \ldots, n$ which is satisfied for all $i$ if $\frac{r}{\upsilon} > \theta$, leading to the second inequality in (14). This completes the proof. ∎

*Remark 5:* The design of gains $\beta, \gamma$ as given in (14) relies on the eigenvalues of $A$, which implies that the network topology has to be known a priori. However, the implementation of control law (7) is distributed since each node makes decisions based on its local and neighbouring information, as evident from (7) and (8).

Finally, the following theorem shows that the approximate leader-follower consensus (4) is ensured in the presence of unknown but bounded attacks.

*Theorem 1:* Consider cooperative system (9) where the communication network topology satisfies assumption 2 and injections $\delta_{ui}(t), \delta_{ji}(t), \bar{\delta}_{ji}(t)$ satisfy assumption 3. Then, for a sufficiently large gains $\beta > 0, \gamma > 0$ satisfying (14), the approximate consensus (4) is ensured for any $\epsilon > 0$.

*Proof:* Let $e(t) = [\tilde{x}^T(t), \tilde{z}^T(t)]^T$ and $\Delta(t) = [(d(t) - \mathbf{1}_n f(x_0(t)))^T, (\bar{d}(t) - \mathbf{1}_n g(z_0(t)))^T]^T$. The error dynamics (13) can be written as

$$\dot{e}(t) = \Phi e(t) + \Delta(t). \tag{15}$$

Since $f(x_0(t)), g(z_0(t)), p^i_{j,1}(t), p^i_{j,2}(t), \delta_{ui}(t), \delta_{ji}(t), \bar{\delta}_{ji}(t)$ are all uniformly bounded, the vector $\Delta(t)$ is also uniformly bounded. The solution to (15) is given by

$$e(t) = \exp(\Phi t)e(0) + \int_0^t \exp(\Phi(t-\tau))\Delta(\tau)d\tau.$$

Let us now compute

$$\lim_{t\to\infty}\|e(t)\| = \lim_{t\to\infty}\left\|\exp(\Phi t)e(0) + \int_0^t \exp(\Phi(t-\tau))\Delta(\tau)d\tau\right\|.$$

Applying Cauchy-Schwartz inequality and by noting from Lemma 1 that $\Phi$ is Hurwitz for gains $\beta, \gamma$ satisfying (14), we have

$$\lim_{t\to\infty}\|e(t)\| \le \lim_{t\to\infty}\left\|\int_0^t \exp(\Phi(t-\tau))\Delta(\tau)d\tau\right\|.$$

Since $\Delta(t)$ is uniformly bounded, there exists a constant vector $\overline{\Delta}$ such that $\|\int_0^t \exp(\Phi(t-\tau))\Delta(\tau)d\tau\| \le \|\int_0^t \exp(\Phi(t-\tau))\overline{\Delta}d\tau\|$. Hence, one can obtain

$$\lim_{t\to\infty}\|e(t)\| \le \lim_{t\to\infty}\left\|\int_0^t \exp(\Phi(t-\tau))\overline{\Delta}d\tau\right\| \le \left\|-\Phi^{-1}\overline{\Delta}\right\|.$$

Matrix $\Phi^{-1}$ can be written as $\Phi^{-1} = \begin{bmatrix}\phi_1 & \phi_2\\ \phi_3 & \phi_4\end{bmatrix}$ where matrices $\phi_1, \phi_2, \phi_3, \phi_4$ are given by $\phi_1 = A^{-1} - \beta^2(\gamma A + \beta^2 A)^{-1}$, $\phi_2 = \beta(\gamma A + \beta^2 A)^{-1}$, $\phi_3 = -\beta(\gamma A + \beta^2 A)^{-1}$, $\phi_4 = (\gamma A + \beta^2 A)^{-1}$ [12]. We can further write them as $\phi_1 = \frac{\gamma}{\beta^2+\gamma}A^{-1}$, $\phi_2 = \frac{\beta}{\beta^2+\gamma}A^{-1}$, $\phi_3 = \frac{-\beta}{\beta^2+\gamma}A^{-1}$, and $\phi_4 = \frac{1}{\beta^2+\gamma}A^{-1}$. Therefore, it can be seen that one can make the error $e(t)$ converges to a small neighbourhood around zero by choosing sufficiently large gains $\beta > 0, \gamma > 0$ satisfying (14). Hence, approximate consensus (4) is ensured. ∎

*Remark 6:* Various control strategies, such as robust control, adaptive control, and observer-based methods, have been proposed in the literature to ensure consensus in the presence of external disturbances, also known as practical consensus. However, these strategies suffer from at least one of the following limitations: (i) the control law depends on the existence of a solution to Linear Matrix Inequalities; (ii) the network's topology is undirected; (iii) the rate of change of the disturbance is bounded; (iv) they do not consider attacks on the communication network when the information being exchanged is corrupted. More importantly, these strategies do not guarantee the privacy of the physical state of the agents. In contrast, the resilient control proposed in our work overcomes all of the above limitations and protects the agents' physical state from eavesdroppers.

### B. Privacy-Preserving Leader-Follower Consensus

Next, we show that the proposed control input (7) and (8) do not only ensure resilient leader-follower consensus in the presence of unknown attacks but also protect the physical states $x_i(t)$ for $i = 0, 1, \ldots, n$ from eavesdropper.

*Proposition 1:* The resilient cooperative control (7), (8) protects the privacy of the node's physical state $x_i(t)$, $i = 0, 1, \ldots, n$ from the eavesdropper.

*Proof:* First, we consider an external adversary. Since the adversary only listens to $y^i_{j,1}(t), y^i_{j,2}(t)$ for $j = 0, 1, \ldots, n$ and does not know the structure of (5)–(8), it is not possible for the adversary to estimate the physical states $x_j(t)$ solely from $y^i_{j,1}(t), y^i_{j,2}(t)$. Next, consider node $i$ who is honest-but-curious and aims to estimate physical state $x_j(t), j \in \mathcal{N}_i \backslash \{0\}$ from the information $y^i_{j,1}(t), y^i_{j,2}(t)$ that it receives. Node $i$ knows the structure of $y^i_{j,1}(t), y^i_{j,2}(t)$ and the values of $\beta$ and $\gamma$ but he/she does not know the values of $z_j(t), p^i_{j,1}(t)$ and $p^i_{j,2}(t)$ which are not shared directly by node $j$. Therefore, in order to learn its neighbouring node's physical state $x_j(t)$ node $i$ has to solve at each time $t$ the underdetermined systems of linear equations given in (5), that is two linear equations with four unknown variables. An underdetermined linear system in general has infinitely many solutions, if any. Hence, it is not possible for the follower node $i$ to accurately estimate the physical state $x_j(t)$. ■

*Remark 7:* An honest-but-curious node will eventually learn about $x_0(t)$ as $x_i(t)$ converges close to $x_0(t)$, see Theorem 1. When there are multiple (but non-cooperative in estimating the physical state) honest-but-curious nodes, as the injections $p^i_{j,1}(t)$, $p^i_{j,2}(t)$ can be designed independently for each link we still have an underdetermined linear system as observed from (5) and thus the privacy can still be ensured. Thorough analysis of multiple curious nodes who aim to cooperatively estimate the physical state is subject to future work.

*Remark 8:* In the absence of attacks, i.e., when $\delta_i(t), \bar{\delta}_i(t)$ are all zero, the physical states $x_i(t)$ do not converge exactly to $x_0(t)$, i.e., $\epsilon > 0$, due to the time varying signals $p^1_{0,1}(t), p^1_{0,2}(t)$ which are not necessarily vanishing asymptotically. The tracking accuracy can then be improved by increasing the gains $\beta$ and $\gamma$.

## IV. A Numerical Example

Consider a cooperative system consisting of four follower nodes ($n = 4$) whose network topology is shown in Fig. 2. In order to better illustrate the results we set $x_0(t) = 2$. Moreover, the dynamics of the attacks in (11) is given by $\dot{\delta}(t) = F_1\delta(t) + B_1 c$ and $\dot{\bar{\delta}}(t) = F_2\bar{\delta}(t) + B_2 c$ where $\delta(t) = [\delta_1(t), \ldots, \delta_n(t)]^T$, $\bar{\delta}(t) = [\bar{\delta}_1(t), \ldots, \bar{\delta}_n(t)]^T$, $F_1 = -I_n$, $F_2 = -0.5I_n$,

$$B_1 = \begin{bmatrix} -1 & 2 & 4 & 2 \\ -4 & 3 & 1 & 2 \\ -3 & 2 & 1 & 1 \\ 2 & 1 & 1 & 2 \end{bmatrix}, B_2 = -B_1, c = 0.2 \times \mathbf{1}_n.$$

It is shown in Fig. 3a that for a standard leader-follower consensus, i.e., by setting $\beta = 0$ in (10), the attacker could prevent the follower nodes from tracking the physical state of the leader node.

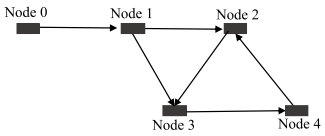


Fig. 2. Cooperative system with four follower nodes.

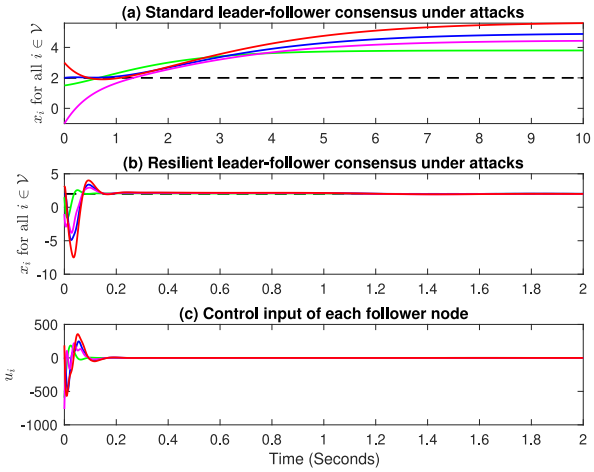


Fig. 3. (a) Standard leader-follower consensus in presence of cyber-attacks. The attacker is able to prevent the follower nodes from tracking the physical state of the leader node; (b) Resilient leader-follower consensus in presence of cyber-attacks. Follower nodes' state converge to a small neighbourhood of state value of the leader under cyber-attacks on the communication links and the actuators. The solid lines denote the trajectories $x_i(t)$ of the follower nodes and the dashed line represents $x_0(t)$; (c) Control input (7) of the follower nodes.

Next, we apply the proposed resilient leader-follower consensus algorithms (7), (8) where the gains are set to $\beta = 95$, $\gamma = 100$. Furthermore, the time-varying signals $p^i_{j,1}(t), p^i_{j,2}(t)$ are set to be a combination of sinusoidal signals of different amplitude, frequency, and phase. Fig. 3b shows the trajectory of the follower nodes. It can be observed that $x_i(t)$, $i = 1, 2, 3, 4$ converge to a small neighbourhood of the leader node's physical state $x_0(t) = 2$. Furthermore, the control input of the follower nodes is shown in Fig. 3c. The control input is mainly affected by the gains $\beta, \gamma$.

Now, let us consider a scenario where an external adversary aims to steal the information of the leader node's physical state $x_0$ by tapping the communication link from the leader node to follower node 1. In order to protect its physical state, instead of sending the physical state $x_0$ the leader node sends the masked state $y^1_{0,1}(t), y^1_{0,2}(t)$ defined in (5) to follower node 1. It can be observed from Fig. 4 that the masked physical state $y^1_{0,1}(t), y^1_{0,2}(t)$ are completely different from $x_0$. Furthermore, even though $x_0$ is constant, the masked information is time varying and does not converge to a constant value. Since the adversary does not know the structure of the masked state in (5) and the time-varying signals $p^1_{0,1}(t), p^1_{0,2}(t)$, it is not possible for the external adversary to learn the physical state $x_0$ from the exchanged information $y^1_{0,1}(t), y^1_{0,2}(t)$.

Finally, assume that node 4 is curious to know the trajectory of node 3. In order to protect its physical state trajectory, instead of sending the physical state $x_3(t)$ node 3 sends the masked state $y^4_{3,1}(t), y^4_{3,2}(t)$ which are different from the true

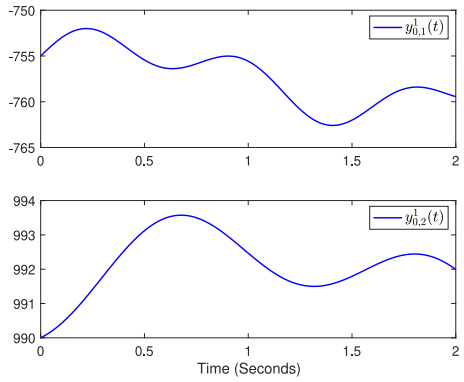


Fig. 4. The information (masked physical state) $y^1_{0,1}(t)$, $y^1_{0,2}(t)$ that leader node sends to follower node 1.

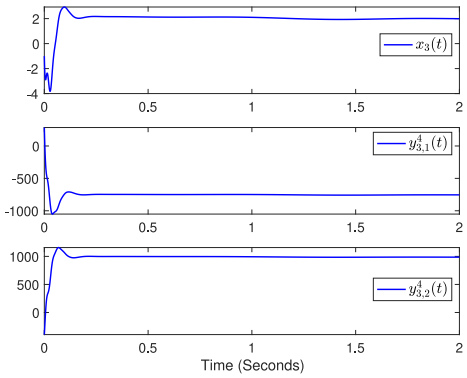


Fig. 5. Instead of sending the true physical state $x_3(t)$, node 3 sends the masked physical state $y^4_{3,1}(t)$, $y^4_{3,2}(t)$ to node 4. Note that the exchanged information are different from the physical state of node 3. Node 4, who is curious, is not able to estimate the physical state of node 3 from the information that it receives as discussed in Section III-B.

state $x_3(t)$ as can be observed from Fig. 5. Since the virtual states $z_3(t)$ and time varying signals $p^4_{3,1}(t), p^4_{3,2}(t)$ are local information of node 3 and are not exchanged with the other nodes, it is not possible for node 4 to estimate $x_3(t)$ from $p^4_{3,1}(t), p^4_{3,2}(t)$ as it needs to solve at each time two linear equations with four unknown variables.

## V. Conclusion and Future Work

This letter proposes a unified control framework that ensures both resilient leader-follower consensus against unknown malicious injections and protection of the physical state of the agents from eavesdropper. The strategy does not require high network connectivity and imposes no restrictions on the number of attacks. Simulation results validate the efficacy of the proposed resilient control algorithm. Future work includes the consideration of input and safety constraints within the proposed resilient control framework.

## References

[1] A. Gusrialdi, Z. Qu, and M. A. Simaan, "Distributed scheduling and cooperative control for charging of electric vehicles at highway service stations," *IEEE Trans. Intell. Transp. Syst.*, vol. 18, no. 10, pp. 2713–2727, Oct. 2017.

[2] J. Hu, P. Bhowmick, F. Arvin, A. Lanzon, and B. Lennox, "Cooperative control of heterogeneous connected vehicle platoons: An adaptive leader-following approach," *IEEE Robot. Autom. Lett.*, vol. 5, no. 2, pp. 977–984, Apr. 2020.

[3] A. Gusrialdi and C. Yu, "Exploiting the use of information to improve coverage performance of robotic sensor networks," *IET Control Theory Appl.*, vol. 8, no. 13, pp. 1270–1283, 2014.

[4] G. Wen, X. Yu, Z.-W. Liu, and W. Yu, "Adaptive consensus-based robust strategy for economic dispatch of smart grids subject to communication uncertainties," *IEEE Trans. Ind. Informat.*, vol. 14, no. 6, pp. 2484–2496, Jun. 2018.

[5] A. Gusrialdi and Z. Qu, "Smart grid security: Attacks and defenses," in *Smart Grid Control: An Overview and Research Opportunities*, J. Stoustrup, A. Annaswamy, A. Chakrabortty, and Z. Qu. Eds. Cham, Switzerland: Springer, 2018, pp. 199–223.

[6] T. Pultarova, "Ukraine grid hack is wake-up call for network operators [news briefing]," *Eng. Technol.*, vol. 11, no. 1, pp. 12–13, Feb. 2016.

[7] F. Pasqualetti, A. Bicchi, and F. Bullo, "Consensus computation in unreliable networks: A system theoretic approach," *IEEE Trans. Autom. Control*, vol. 57, no. 1, pp. 90–104, Jan. 2012.

[8] A. Eslami, F. Abdollahi, and K. Khorasani, "Stochastic fault and cyber-attack detection and consensus control in multi-agent systems," *Int. J. Control*, vol. 5, no. 9, pp. 2379–2397, 2022.

[9] J. Usevitch and D. Panagou, "Resilient leader-follower consensus to arbitrary reference values in time-varying graphs," *IEEE Trans. Autom. Control*, vol. 65, no. 4, pp. 1755–1762, Apr. 2020.

[10] H. Rezaee, T. Parisini, and M. M. Polycarpou, "Resiliency in dynamic leader–follower multiagent systems," *Automatica*, vol. 125, Mar. 2021, Art. no. 109384.

[11] M. S. Sadabadi and A. Gusrialdi, "On resilient design of cooperative systems in presence of cyber-attacks," in *Proc. Eur. Control Conf.*, Rotterdam, The Netherlands, 2021, pp. 946–951.

[12] M. Iqbal, Z. Qu, and A. Gusrialdi, "Distributed resilient consensus on general digraphs under cyber-attacks," *Eur. J. Control*, vol. 68, Nov. 2022, Art. no. 100681.

[13] A. Gusrialdi, Z. Qu, and M. A. Simaan, "Competitive interaction design of cooperative systems against attacks," *IEEE Trans. Autom. Control*, vol. 63, no. 9, pp. 3159–3166, Sep. 2018.

[14] J. Wang, Y. Li, Z. Duan, and J. Zeng, "A fully distributed robust secure consensus protocol for linear multi-agent systems," *IEEE Trans. Circuits Syst. II, Exp. Briefs*, vol. 69, no. 7, pp. 3264–3268, Jul. 2022.

[15] L. Wang, C. Fan, C. Xie, and W. Zhou, "Leader-following consensus of multiple Euler-Lagrange systems under deception attacks," *IEEE Access*, vol. 9, pp. 100548–100557, 2021.

[16] Z. Zuo, X. Cao, Y. Wang, and W. Zhang, "Resilient consensus of multiagent systems against denial-of-service attacks," *IEEE Trans. Syst., Man, Cybern., Syst.*, vol. 52, no. 4, pp. 2664–2675, Apr. 2022.

[17] H. Xu, Y.-H. Ni, Z. Liu, and Z. Chen, "Privacy-preserving leader-following consensus via node-augment mechanism," *IEEE Trans. Circuits Syst. II, Exp. Briefs*, vol. 68, no. 6, pp. 2117–2121, Jun. 2021.

[18] M. Ruan, H. Gao, and Y. Wang, "Secure and privacy-preserving consensus," *IEEE Trans. Autom. Control*, vol. 64, no. 10, pp. 4035–4049, Oct. 2019.

[19] C. Ying, N. Zheng, Y. Wu, M. Xu, and W.-A. Zhang, "Privacy-preserving adaptive resilient consensus for multi-agent systems under cyber attacks," *IEEE Trans. Ind. Informat.*, early access, May 26, 2023, doi: 10.1109/TII.2023.3280318.

[20] D. Fiore and G. Russo, "Resilient consensus for multi-agent systems subject to differential privacy requirements," *Automatica*, vol. 106, pp. 18–26, Aug. 2019.

[21] Z. Qu and M. A. Simaan, "Modularized design for cooperative control and plug-and-play operation of networked heterogeneous systems," *Autmatica*, vol. 50, no. 9, pp. 2405–2414, Sep. 2014.

[22] X. Huang and J. Dong, "Reliable cooperative control and plug-and-play operation for networked heterogeneous systems under cyber–physical attacks," *ISA Trans.*, vol. 104, pp. 62–72, Sep. 2020.

[23] R. Gao and J. Huang, "Leader-following consensus of uncertain strict feedback multiagent systems subject to sensor and actuator attacks," *Int. J. Robust Nonlinear Control*, vol. 30, no. 17, pp. 7635–7654, 2020.

[24] M. Shi, X. Chen, M. Shahidehpour, Q. Zhou, and J. Wen, "Observer-based resilient integrated distributed control against cyberattacks on sensors and actuators in islanded AC microgrids," *IEEE Trans. Smart Grid*, vol. 12, no. 3, pp. 1953–1963, May 2021.

[25] A. Mustafa and H. Modares, "Attack analysis and resilient control design for discrete-time distributed multi-agent systems," *IEEE Robot. Autom. Lett.*, vol. 5, no. 2, pp. 369–376, Apr. 2020.

[26] Z. Qu, *Cooperative Control of Dynamical Systems*. London, U.K.: Springer, 2009.